



TASK ORDER REQUEST (TO) 47QFCA19F0040 P00003

United States Army Open-Source Intelligence Capabilities (AOC)

in support of:

United States Army Intelligence and Security Command



Awarded to:

**BAE Systems Technology Solutions & Services, Inc. under the General Services
Administration (GSA) One Acquisition Solution for Integrated Services (OASIS) Multiple
Award (MA) Indefinite Delivery/Indefinite Quantity (IDIQ) – Unrestricted Pool 1 Contract
GS00Q14OADU103**

Conducted under Federal Acquisition Regulation (FAR) 16.505

Awarded by:

**The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405**

October 18, 2019

FEDSIM Project Number 2019-35055

C.1 BACKGROUND

The United States (U.S.) Army Intelligence and Security Command (INSCOM), an Army Direct Reporting Unit (DRU), executes mission command of operational intelligence and security forces; conducts and synchronizes worldwide multi-discipline and Open Source Intelligence (OSINT) and security operations; and delivers linguist support and intelligence-related advanced skills training, acquisition support, logistics, communications, and other specialized capabilities in support of Army, Joint, and Coalition Commands and the U.S. Intelligence Community (IC). INSCOM is a global command with multiple Major Subordinate Commands (MSCs). INSCOM is the Army-wide OSINT program manager including INSCOM organizations, U.S. Army Forces Command (FORSCOM) and its subordinate Military Intelligence (MI) elements, Army Special Operations Forces and its subordinate MI elements, as well as other Army Service Component Commands (ASCCs), Army Commands (ACOMs), intelligence and intelligence-related activities, and partners/foreign partners approved by the Army OSINT Office (AOO). In January 2016, Headquarters Department of the Army (HQDA) validated the Army Global OSINT requirements. All further references to INSCOM throughout this document include its MSCs and other subordinate units located in the U.S and deployed overseas.

C.1.1 PURPOSE

The purpose of this TO is to operationalize OSINT to the Department of the Army, ASCC, and other Major ACOMs in support of Conventional and Special Operations Forces. This activity will inform and implement Army policy and provide access to, training for, and management and oversight of enterprise-approved OSINT capabilities for the Army. This TO will provide OSINT capabilities that meet the Army's demands and requirements. This TO will also provide limited tool and training support as approved by the AOO to Counter-Intelligence (CI) personnel, non-intelligence personnel, and foreign intelligence partners conducting like activities, as needed.

C.1.2 AGENCY MISSION

The AOO is responsible for the expansion of existing and emerging capabilities deemed essential to enable Army MI elements and AOO approved partners supporting theater and functional Combatant Commands (CCMDs) in the use of Publically Available Information (PAI) for intelligence or intelligence-related purposes. The AOO operationalizes OSINT collection capabilities in support of Conventional and Special Operations Forces. The AOO executes requirements for, training of, and access to capabilities provisioned by its Defense and National OSINT partners, facilitating on-demand, near real-time intelligence collection for unit commanders and theater decision-makers.

AOO is charged to conduct operations that were not envisioned or resourced during its organizational design and development; it approaches its mission by focusing efforts on:

- a. Operationalizing and professionalizing advanced OSINT collection and exploitation through training.
- b. Supporting OSINT teams Army-wide.
- c. Serving as the Army OSINT Capabilities Manager.
- d. Managing requirements for and access to capabilities.
- e. Budgeting for essential resources to enable in the Program's successful execution.

SECTION C – PERFORMANCE WORK STATEMENT

- f. Auditing for Intel Oversight Compliance in accordance with Department of Defense Manual (DoDM) 5240.01.
- g. Informing policy and doctrine.

C.2 SCOPE

The scope of this TO is to support the expansion of existing and emerging OSINT capabilities. This support includes the activities related to and in support of delivering collection and exploitation support, training, capabilities management support, OSINT readiness, hosting environment support services, and emergent project support as needed.

Performance of services will be at multiple locations in the Continental United States (CONUS) and Outside the Continental United States (OCONUS) including, but not limited to the locations in Section F. Extensive CONUS and OCONUS travel is expected.

C.3 CURRENT OPERATING ENVIRONMENT

INSCOM provides on-going OSINT capability and training across the globe to the Department of the Army, ASCC, and other Major ACOMs. The Areas of Responsibility (AOR) that make up the current operating environment include, but are not limited to, the following:

- a. U.S. Army FORSCOM and its subordinate organizations.
- b. U.S. Africa Command (AFRICOM) and U.S. Army Africa (USARAF).
- c. U.S. Indo-Pacific Command (USINDOPACOM) and U.S. Army Pacific (USARPAC).
- d. U.S. Special Operations Command (SOCOM), Army Special Operations Command (USASOC), and subordinate commands.
- e. U.S. European Command (EUCOM) and U.S. Army Europe (USAREUR).
- f. U.S. Northern Command (NORTHCOM), U.S. Army North (USARNORTH), U.S. Southern Command (SOUTHCOM), and U.S. Army South (USARSOUTH).
- g. Army National Guard (ARNG.)
- h. Army Reserve Intelligence Support Centers (ARISCs) and Joint Reserve Intelligence Centers (JRICs).

Detailed information on the current OSINT environment can be found in Section J, Attachment W.

C.4 OBJECTIVE

The objectives of this effort are to:

- a. Sustain, enhance, and automate INSCOM's ability to collect and exploit PAI in an innovative, timely, and cost-effective manner.
- b. Enhance the synergies between INSCOM and the other major entities in the IC to keep pace with evolving threats through continuous innovation of OSINT capabilities.
- c. Enhance INSCOM's ability to store and exploit large data sets beyond the current capabilities using big data analytics, in order to facilitate faster and more streamlined decision making.
- d. Continue to be a leader in OSINT tradecraft training.

SECTION C – PERFORMANCE WORK STATEMENT

- e. Provide and sustain a hosting environment that allows for Single Sign-On (SSO) access to the OSINT Toolkit 24 hours per day, seven days per week, and 365 days per year (24x7x365).
- f. Support an innovative, timely, and cost-effective approach to technology assessments of existing OSINT/PAI capabilities and emerging technologies.
- g. Ensure that the capabilities and practices conducted by the AOO reduce or mitigate the OSINT challenges in the safest, most efficient, and cost-effective manner.
- h. Ensure solution delivery aligns with the AOO Director's program priorities and AOO's operational goals and mission.
- i. Provide quick, innovative, and cost-effective response to support urgent operational needs and emergent projects.

C.5 TASKS

The major task areas of the Army OSINT Capabilities (AOC) TO are defined below:

- Task 1 – Program Management
- Task 2 – Collection and Exploitation Support
- Task 3 – Training
- Task 4 – OSINT Capabilities Management
- Task 5 – OSINT Readiness
- Task 6 – OSINT Hosting Environment
- Task 7 – Emergent Project Support (Optional)

C.5.1 TASK 1 – PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors and teaming partners, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall provide the required OSINT support services for a number of locations across CONUS and OCONUS.

C.5.1.1 SUBTASK 1 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for INSCOM via a secure data collection site: the Enterprise Contractor Manpower Reporting Application (ECMRA). The contractor shall completely fill in all required data fields using the following web address: <http://www.ecmra.mil/>.

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported No Later Than (NLT) October 31 of each calendar year. Contractors may direct questions to the support desk at: <http://www.ecmra.mil/>.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a

SECTION C – PERFORMANCE WORK STATEMENT

contractor's systems to the secure website without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.5.1.2 SUBTASK 2 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at the location approved by the Government (Section F, Deliverable 01). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the directorates, other relevant Government personnel, and the FEDSIM COR.

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (Section F, Deliverable 02) for review and approval by the FEDSIM COR and the INSCOM Technical Point of Contact (TPOC) prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

- a. Points of contact (POCs) for all parties.
- b. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
- c. Project Staffing Plan and status.
- d. Transition-In Plan (Section F, Deliverable 14) and discussion.
- e. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs)).
- f. Invoicing requirements.
- g. Baseline Quality Management Plan (QMP) (Section F, Deliverable 11).
- h. Technical Direction Plans (TDPs)
- i. Status and process of the following OCONUS Special Requirements: Theater Business Clearance (TBC), Letters of Authorization (LOA), Government-Furnished Life Support Validation (GFLSV), Synchronized Predeployment and Operational Tracker (SPOT), Technical Expert Status Accreditation (TESA), and Status of Forces Agreement (SOFA).

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting, and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Minutes Report (Section F, Deliverable 03) documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.3 SUBTASK 3 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (Section F, Deliverable 04). The MSR shall include the following:

- a. Activities during reporting period, by task (include on-going activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task.

SECTION C – PERFORMANCE WORK STATEMENT

- b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- c. Personnel gains, losses, and status (security clearance, etc.).
- d. Government actions required.
- e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
- g. Cost incurred by CLIN.
- h. Accumulated invoiced cost for each CLIN up to the previous month.
- i. Projected cost of each CLIN for the current month.
- j. Status of TDPs and Technical Direction Letters (TDLs)
 - 1. Details on schedule, staffing levels, and progress of performance.
 - 2. Details on cost incurred by CLIN (i.e., labor, travel, tools, CAF, and ODCs), line of accounting, accumulated invoiced cost for TDP/TDL up to the previous month, and projected cost of each CLIN for current month.
 - 3. Issues, concerns, and opportunities.

The contractor shall prepare the MSR using the sample MSR template provided in Section J, Attachment F.

C.5.1.4 SUBTASK 4 – CONVENE TECHNICAL STATUS MEETINGS

The contractor Program Manager (PM) shall convene a monthly Technical Status Meeting with the INSCOM TPOC, FEDSIM COR, and other Government stakeholders (Section F, Deliverable 05). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities such as TDPs/TDLs and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR (Section F, Deliverable 06).

C.5.1.5 SUBTASK 5 – PREPARE PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The contractor shall provide the Government with a draft PMP (Section F, Deliverable 07) on which the Government will make comments. The final PMP (Section F, Deliverable 08) shall incorporate the Government's comments.

The PMP shall:

- a. Describe the proposed management approach.
- b. Contain detailed Standard Operating Procedures (SOPs) for all tasks.
- c. Include milestones, tasks, and subtasks required in this TO.
- d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.
 - 1. The WBS shall identify all technical activities at a level of detail sufficient for the contractor to manage the work.

SECTION C – PERFORMANCE WORK STATEMENT

2. Each WBS element shall be accompanied by a description and expected result(s).
3. Each WBS element shall include an estimate of the level of effort required by labor category and associated cost.
- e. Describe in detail the contractor's approach to risk management under this TO.
- f. Describe in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government.
- g. Describe in details the contractor's approach to the management of TDPs and TDLs from inception to closeout.
- h. Describe in detail the contractor's approach for OCONUS special requirements such as TBC, LOAs, GFLSV, SPOT, TESA, and SOFA.
- i. Include the contractor's QMP.

C.5.1.6 SUBTASK 6 – UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated annually at a minimum (Section F, Deliverable 09). The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.7 SUBTASK 7 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted (Section F, Deliverable 10). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, trip reports shall be prepared with the information provided in Section J, Attachment G.

C.5.1.8 SUBTASK 8 - PREPARE TECHNICAL DIRECTION PLANS (TDPs)

TDPs are a means of clarifying contractual requirements or direction of a technical nature, within the context of the TO. The contractor shall prepare TDPs in response to an approved FEDSIM Contracting Officer (TDL) in accordance with **Section H.19**. The contractor shall tailor the requirements for each TDP. The TDP is an evolutionary document and the contractor shall work from the latest Government-approved version of the TDP.

The TDP shall include:

- a. Project overview.
- b. Project cost estimate (Rough Order of Magnitude (ROM)).
- c. Master Equipment List (MEL)/Bill of Materials (if applicable).
- d. Project schedule including milestones, tasks, and subtasks required in this project.
- e. Project risks and mitigations.
- f. Project staff and resources.
- g. Performance criteria.
- h. Travel considerations.
- i. Project work products deliverables.

SECTION C – PERFORMANCE WORK STATEMENT

- j. Security considerations.
- k. Provide for an overall WBS.
- l. Project transition.
- m. TDP customer feedback participation.

The contractor shall host a Project Kick-Off Meeting for each approved TDL and shall provide a meeting agenda and meeting minutes.

C.5.1.9 SUBTASK 9 – PROVIDE QUALITY MANAGEMENT

The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the TO. The contractor's QMP shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The QMP shall describe how the appropriate methodology integrates with the Government's requirements.

The contractor shall provide a baseline QMP as required in Section F (Section F, Deliverable 12). The contractor shall periodically update the QMP, as required in Section F (Section F, Deliverable 13), as changes in program processes are identified.

C.5.1.10 SUBTASK 10 – TRANSITION-IN

The contractor shall update the draft Transition-In Plan (Section F, Deliverable 14) provided with its proposal and provide a final Transition-In Plan as required in Section F (Section F, Deliverable 15). The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The tools and capabilities identified in Section J, Attachment X shall be available for performance NLT 135 days after project start. The aforementioned tools and capabilities have various expiration dates for their support, and must be in place in this time period to ensure continued performance. The contractor shall implement its Transition-In Plan NLT ten calendar days after project start, and all transition activities shall be completed 60 calendar days after approval of final Transition-In Plan (Section F, Deliverable 15).

C.5.1.11 SUBTASK 11 – TRANSITION-OUT

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a draft Transition-Out Plan within six months of Project Start (PS) (Section F, Deliverable 16). The Government will work with the contractor to finalize the Transition-Out Plan (Section F, Deliverable 17) in accordance with Section E. At a minimum, the Transition-Out Plan shall be reviewed and updated on an annual basis (Section F, Deliverable 18). Additionally, the Transition-Out Plan shall be reviewed and updated quarterly during the final Option Period (Section F, Deliverable 18).

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

- a. Project management processes.
- b. POCs.

SECTION C – PERFORMANCE WORK STATEMENT

- c. Location of technical and project management documentation.
- d. Status of ongoing technical initiatives.
- e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
- f. Transition of Key Personnel.
- g. Schedules and milestones.
- h. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

C.5.2 TASK 2 – COLLECTION AND EXPLOITATION SUPPORT

The contractor shall conduct the collection and exploitation of PAI by providing access to an AOO-approved suite of tools to answer both standing and ad hoc data intelligence requirements in a timely manner, as required by the time sensitivity of the requirement. The contractor shall use its collection and exploitation of PAI to prepare ad hoc responses to requirements or Open Source Intelligence Reports (OSIR), along guidelines standardized by Defense and Intel Communities. The contractor shall assist soldiers, civilians, and contractors in Army Intel roles to conduct critical tasks in research, collection, production, exploitation, and dissemination of OSINT products, as needed.

Intelligence exploitation shall include OSINT in support of other intelligence disciplines, such as All Source Intelligence, Signals Intelligence (SIGINT), Geospatial Intelligence (GEOINT), and Counterintelligence/Human Intelligence (CI/HUMINT), as well as specialized skills (e.g., open source support to counter terrorism, cyber threat analysis, cyber operations, information operations and other disciplines) that may develop during the life of this contract. The contractor shall process, translate (if applicable), develop, and exploit the data to produce OSIR (Section F, Deliverable 19) and other supplemental deliverables as determined by the supported commander. If collection of PAI reveals an imminent force protection threat, the contractor shall immediately notify appropriate law enforcement, CI organization, or other appropriate Government entity. The contractor shall develop and maintain collection and exploitation procedures to meet changing requirements and ensure maximum operational success.

C.5.2.1 SUBTASK 1 – LINGUISTIC CAPABILITY

The contractor shall increase the organic linguistic capabilities of the AOO. The contractor shall increase the language proficiency of Government personnel associated with Task 2 – Collection and Exploitation Support, to at least at the +2 level on the Defense Language Proficiency Test (DLPT) or equivalent. The Government will provide direction on the applicable languages for each location post-award. The contractor shall develop a draft Linguistic Capability Plan (LCP) (Section F, Deliverable 20). Once the Government has provided comments/feedback, the contractor shall respond and incorporate the comments/changes and provide a final LCP (Section F, Deliverable 21). The contractor shall execute the LCP in accordance with Government direction. The contractor shall provide LCP updates (Section F, Deliverable 22), to implement requirements, and continue to tailor the plan to the Government's needs.

C.5.3 TASK 3 – TRAINING

C.5.3.1 SUBTASK 1 – MOBILE TRAINING TEAM (MTT)

The contractor shall train soldiers, civilians, and contractors in the collection and exploitation of PAI, OSINT reporting, dissemination, and coordination or cueing other intelligence disciplines. The contractor shall frequently travel to CONUS and OCONUS locations.

The contractor shall conduct training of OSINT Programs of Instruction (POI) approved by the AOO and support the development of new/revised curricula to maintain POI currency. The contractor's POI shall include, but are not limited to, the following:

- a. Refreshers as needed on OSINT fundamentals.
- b. Real-time event detection and alerting.
- c. PAI Collection with secure browsing techniques and dark web exploitation.
- d. Procedures for accessing deep web (data acquisition).
- e. Focused in-depth exploitation and data visualization).
- f. Machine language translation of foreign language media content.
- g. Procedures for applying for access to Department of Defense (DoD) enterprise-level approved tools and programs.
- h. Collection requirement management.
- i. Procedures for complying with Open Source Intelligence Reporting (OSIR) requirements.
- j. Computer and mobile device security
- k. Deep understanding of PAI and databases available to Army/DOD enterprise users

In addition to the POI, the contractor shall:

- a. Seek continued relevance on new internet data sets and exploitation tools.
- b. Conduct training and develop criteria for evaluating the effectiveness of training activities.
- c. Develop, organize, and conduct training and educational programs for approved Army personnel.
- d. Provide research for national security, infrastructure, technology, country, geographic area, and biographic and targeted vulnerability.
- e. Establish and review course content and objectives to ensure a well-integrated and unified OSINT training program.
- f. Maintain records of training activities, participant progress, and program effectiveness.
- g. Update course documentation on a regular basis to ensure timeliness and relevance.
- h. Provide innovative learning solutions and apply industry best practices to address unique training challenges.
- i. Conduct research into new training, educational, and multimedia technologies.
- j. Maintain current knowledge of relevant technologies and subject areas.
- k. Describe the capabilities and limitations of current and future PAI collection and exploitation technologies.

SECTION C – PERFORMANCE WORK STATEMENT

C.5.3.2 SUBTASK 2 – TRAINING COORDINATION AND OUTREACH

The contractor shall provide administrative and logistical support in support of MTTs at INSCOM Headquarters (HQ).

The contractor shall process requests for OSINT training from across the U.S. Army enterprise and other AOO-approved customers, scheduling the training based on the availability of the AOO training personnel and reviewing unit's mission requirements.

The contractor shall prepare schedules, rosters, Virtual Teleconference (VTC) reservations, and other scheduling support in advance of the MTT, and be available during MTT execution to resolve issues related to the planning and execution of the MTT. Once an MTT has been completed, the contractor shall receive post-training materials from the trainers and input appropriate data into AOO databases to maintain an audit trail of all training conducted. Before, during, and after MTT execution, the contractor shall support the creation or deletion of accounts to PAI collection and exploitation tools based on the eligibility of the intelligence professionals as recorded in AOO databases.

The contractor shall support the quarterly audit of all AOO approved users with access to AOO provisioned capability by communicating with appropriate unit POCs and either provisioning or removing access, as necessary, based on those audits. The contractor shall prepare ad-hoc reports, graphs, charts, and presentations required to conduct and facilitate all training activities. The contractor shall regularly communicate with supported units, other directorates, other services, vendors, and agencies in-person, by phone, and via email, acting as the primary entry point for AOO engagements. The contractor shall assist in developing new methods for tracking and reporting AOO program statistics, maintaining key customer information, and improving upon existing standards and processes.

C.5.3.3 SUBTASK 3 – PROGRAM OF INSTRUCTION (POI) REFINEMENT

C.5.3.3.1 TRAINING SUPPORT PACKAGE (TSP) MAINTENANCE AND REVIEW

The contractor shall deliver training products, participate in training product development sessions, and instruct training classes. In order to support this, the contractor shall develop TSPs (Section F, Deliverable 23) in accordance with Government requirements. The TSPs shall maintain the current training curriculum at each location. The contractor shall maintain all applicable POI, Lesson Plans, Practical Exercises, and Evaluations. The contractor shall deliver the instruction in accordance with the training Analysis, Design, Development, Implementation, and Evaluation (ADDIE) process concepts.

The contractor shall convene TSP Reviews (Section F, Deliverable 24) on a semi-annual basis or at Government request. The objective of the TSP is to assess the current training curriculum at each location/organization in scope of this contract and to assess documentation, across the contract, and its effectiveness based on After Action Reviews (AARs), lessons learned, and other applicable sources. The contractor shall stay abreast of the current status of policy and doctrine, as significant changes to the TSP may occur if there is a change to either. As changes occur, the contractor shall make recommendations (Section F, Deliverable 25) and changes to the TSP after Government approval.

C.5.4 TASK 4 - OSINT CAPABILITIES MANAGEMENT

The contractor shall provide technology assessments of existing OSINT/PAI capabilities and emerging technologies. The contractor shall provide recommendations for integration into the OSINT Toolkit (Section F, Deliverable 26). The recommendation shall include a business case analysis that evaluates the viability of the tool, a cost benefit analysis, a recommendation for utilizing the testing and evaluation environment, and a plan for moving the tool directly to the operational environment (if applicable). Capability Management Support (CMS) shall also conduct analysis of current tools and support the removal of OSINT and PAI collection, exploitation, visualization, dissemination, and alerting technologies in a rapid manner. The contractor shall provide the rapid acquisition of accounts or removal of accounts based on the needs of the enterprise.

C.5.4.1 SUBTASK 1 – CAPABILITY MANAGEMENT SUPPORT (CMS)

CMS directly supports the AOO director's intent by providing capabilities and analysis that enables the AOO leadership to address the gaps, overlaps, and possible duplication effort at the enterprise-level rather than at the individual operator's level. CMS shall include, but is not limited to, the following:

- a. Coordinate and represent the AOO on the appropriate DoD and National-level standard-setting bodies and organizations and requirements and capabilities boards and working groups.
- b. Work closely with the AOO components to ensure programs and systems reduce or mitigate the challenges in the safest, most efficient, and most cost-effective manner.
- c. Advise on requirements and planning for acquisitions, ensuring OSINT technologies are reliable, interoperable, and effective.
- d. Use technical and analytic techniques to identify and prioritize capability gaps and find solutions for Army OSINT operations.
- e. Provide accessing and recommending oversight for all OSINT tools and subscription services as well as in evaluating collection and analysis technologies.
- f. Provide an innovative, systems-based approach to help operators define their needs and develop technologies and solutions that can be quickly deployed to frontline operators.
- g. Define requirements from a project's inception to conclusion for complex to extremely complex programs.
- h. Provide strategic advice, technical guidance, and expertise to program and project staff.
- i. Provide detailed analysis and recommendations for improvements, optimization development, and/or maintenance efforts for client-specific or mission-critical challenges/issues.
- j. Consult with the client to define the need, problem, and solution. Lead studies and surveys to collect and analyze data to provide advice and recommend solutions.
- k. Explore emerging capabilities in Big Data, Data Analytics, and Data Science to support definition of AOO Data Strategy.
- l. Prepare assessments of current threats and trends based on the sophisticated collection, research, and analysis of classified and open source information.

SECTION C – PERFORMANCE WORK STATEMENT

C.5.5 TASK 5 – OSINT READINESS

The contractor shall provide the functional support required to maximize operational OSINT readiness. The contractor shall interpret higher authority direction, command guidance, and strategies to accomplish the Director's MI priorities as reflected in the operational goals and missions. The contractor shall provide oral and written recommendations for the general officer level audiences on multi-year projects, doctrine, and policies that will affect the entire Army. The contractor shall provide input to graphic and visual products for presentation to senior officers, as well as edit and coordinate the final drafting of documents and graphic presentations (Section F, Deliverable 27), from other members of the AOO team, prior to submission as the approved position of the AOO and/or HQ INSCOM, as required. The contractor shall provide the following senior level support activities:

- a. Conduct research, analysis, and coordination of strategy, policy, and doctrine at the IC, DoD, Service, and Command levels.
- b. Executive-level projects and analyze, assess, and develop future strategy and guidance governing Army OSINT operations.
- c. IC, DoD, and interagency policy formulations on OSINT issues and foreign partner agreements, ensuring authorities, concerns, and AOO equities are accurately represented.
- d. Conduct research to support and provide strategic and conceptual guidance to IC leaders.
- e. Conduct novel and systematic analyses of the tasking, collection, exploitation, and dissemination of OSINT.
- f. Conduct data assembly and analysis; participate in focus groups; prepare draft documents and presentations; and coordinate work among project team members.
- g. Intelligence and information sharing and safeguarding integration and coordination efforts.
- h. Provide support IC issues through interaction and collaboration with appropriate mission partners.
- i. Advise and support advancement of key intelligence and information sharing projects, ensuring proper agency coordination is completed in a timely and effective matter.

C.5.5.1 SUBTASK 1 – OVERSIGHT AND COMPLIANCE ACTIVITY

The contractor shall conduct OSINT Activity Audits (Section F, Deliverable 28) at INSCOM HQ at Fort Belvoir, VA, in accordance with DoD Manual (DoDM) 5240.01, dated August 2016; Secretary of the Army (SECARMY) Directive 2016-37, dated 17 November 2017; and INSCOM Operation Order (OPORD) 17-132. The contractor shall ensure compliance with these requirements and perform audits on 100 percent of the key log files for all Army accounts. The contractor shall perform the audits by trained specialists and comply with the published and posted schedule. The auditor uses designated scripts to search each audited account focusing on improper use according to AOO policy. The auditor shall review the log search results to compile the findings based on results from dirty word lists, unauthorized domains, and behavior not compliant with the AOO Managed Attribution Terms of Use (TOU) and Army Regulation (AR) 381-10.

The auditor shall maintain key logs on a shared drive using an agreed upon naming convention and made available to investigators for further scrutiny and reference in the case of potential Questionable Intelligence Activities (QIAs) reporting or TOU violations. Potential QIAs and/or

SECTION C – PERFORMANCE WORK STATEMENT

misuse shall be reported and require additional searches of person(s) identified as possibly performing unauthorized activity. The objective of the additional searches is to identify either a pattern or history of misconduct, if any. The AOO auditor shall provide additional background information on the user's activity on the managed attribution system to the Intelligence Oversight Office or designated investigators, as necessary. The AOO auditor shall be readily available to further assist the Intelligence Oversight Office and/or investigator and respond for any additional information that may be requested.

C.5.5.2 SUBTASK 2 – SIGNATURE REDUCTION

The contractor shall maintain knowledge of established Signature Reduction plans to ensure they support current and future operations. The contractor shall utilize appropriate Signature Reduction methodologies in the provision of this staff and operations support. The Government will provide training and direction in the execution of these methodologies. The contractor shall support the request, management, and deactivation of required Signature Reduction mechanisms and support. In addition to this, the contractor shall perform organizational, individual, and operational due diligence in accordance with DoD policies to maintain plans, mechanisms, and travel awareness. The contractor shall assist with periodic Command inspections of subordinate units for Signature Reduction-related programs, assist in determining operational validity and review of subordinate element Signature Reduction plans, and evaluate the sustainability of the unit's Signature Reduction Tactics, Techniques, and Procedures (TTPs).

The contractor shall draft responses to Signature Reduction requirements and assigned projects, and engage associated organizations for support and collaborating or coordinating on externally generated requirements. The contractor shall review and refine Signature Reduction programs and/or SOPs, and other regulatory documents to ensure compliance with DoD policies and regulations.

C.5.5.2.1 SIGNATURE REDUCTION TRAINING

The contractor shall prepare and deliver Signature Reduction training for Soldiers, civilians, and contractors in support of unit readiness. The contractor shall ensure that training is relevant to the operational and administrative needs of Signature Reduction and reflects the current approved Signature Reduction tradecraft.

C.5.6 TASK 6 – OSINT HOSTING ENVIRONMENT

The contractor shall provide an OSINT hosting environment that supports a testing and operational capability. This OSINT hosting environment shall support an OSINT toolkit, utilize a SSO system, and operate on unclassified DoD networks. The contractor shall operate and maintain the OSINT Hosting environment.

This shall include, but is not limited to, the following:

- a. Provide day to day access to a suite of tools used to collect, search, and exploit publicly available data.
- b. Scale (buying more or less accounts) access to tools up or down periodically based on enterprise need.
- c. Provide administrative access on platform to support creation/deletion of accounts and access to tools by staff, auditors, and trainers.

SECTION C – PERFORMANCE WORK STATEMENT

- d. Conduct evaluating, researching, and testing of new tools for integration into environment at request of Government.
- e. Ensure the rapid integration and deployment of innovative plug-and-play technologies.
- f. Provide environment architecture that delivers authentication, end-user access, security, auditing, compliance, and dynamic system scaling support.
- g. Provide the capability for hosting and dissemination of unclassified//For Official Use Only (FOUO) information with access constraints, encryption at rest and in-transit standards, ingest, data partitioning and handling, analytics, and management of data up to any standard developed by executive agencies in accordance with Executive Order 13556 – Controlled Unclassified Information.

C.5.6.1 SUBTASK 1 – OSINT PLATFORM SUPPORT

The contractor shall provide a secure, web-accessible, commercially-hosted platform that supports operational and testing environments for current and emerging OSINT and PAI collection, exploitation, visualization, dissemination, and alerting technologies. The platform must be flexible and scalable to meet the requirements of all users and organizations. The platform must also have layered permissions to include user roles and administrative roles that support the maintenance of user roles (e.g., creation, deletion, provisioning of tools and services, and other necessary actions). There shall also be 24x7x365 technical support at Tiers 1, 2, and 3 available to ensure no loss of capability or access. In the event that a service disruption is unavoidable, the contractor shall inform the Government no less than two weeks in advance, and the system shall not be unavailable for longer than two hours. These interruptions shall not occur more than once per quarter.

C.5.6.1.1 – PLATFORM OPERATIONAL ENVIRONMENT

The contractor shall provide an unclassified, “Federal Risk and Authorization Management Program (FedRAMP) approved for FOUO data” operational environment in which users can access any provisioned tools or services with appropriate permissions. FedRAMP is a Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This must include R Code for user-defined web scraping and the integration of AOO-approved collection and exploitation Commercial Off-the-Self (COTS) tools. This environment must be secure, not directly attributable to U.S. Government (USG) or DoD networks. It also must provide remote access from regions across the globe and require neither physical installation of hardware nor the installation of software on client endpoints.

The contractor shall provide a platform capable of moving approved OSINT and PAI collection, exploitation, visualization, dissemination, and alerting tools from the testing environment to the operational environment at the completion of test and evaluation activities. The platform shall also support the direct integration of approved tools and services at the request of the Government, regardless if they have been housed in the testing environment.

C.5.6.2 SUBTASK 2 – OSINT TOOLKIT

The contractor shall provide a platform to host an OSINT Toolkit integrated with the operational environment. The Toolkit must be flexible and support the addition or removal of OSINT and PAI collection, exploitation, visualization, dissemination, and alerting technologies in a rapid

SECTION C – PERFORMANCE WORK STATEMENT

manner. The Toolkit must also be scalable and allow for the addition or deletion of accounts on tools and services approved for use on the platform in a rapid manner. This includes the rapid acquisition of accounts or removal of accounts based on the needs of the enterprise. The Toolkit must be secure, not directly attributable to USG or DoD networks. It also must provide remote access from regions across the globe and require neither physical installation of hardware, nor physical installation of software on client endpoints. There shall also be 24x7x365 technical support at Tiers 1, 2, and 3 available to ensure no loss of capability or access. In the event that a service disruption is unavoidable, the contractor shall inform the Government no less than two weeks in advance, and the system shall not be unavailable for longer than two hours. These interruptions shall not occur more than once per quarter. The platform shall be accredited for FOUO by FedRAMP and a SSO function shall reside within the Toolkit.

The contractor shall provide support for custom toolkit requirements and systems in the form of short-term projects and initiatives and for unanticipated requirements including DoD and Congressional mandates.

C.5.7 TASK 7 – EMERGENT PROJECT SUPPORT (OPTIONAL)

Unpredictable world events demand that INSCOM have the capability to maintain quick responsiveness to unscheduled fieldings and tactical units worldwide to support the warfighter and sustain National Security. Accordingly, the contractor shall provide quick reaction support in response to emergent special projects.

This additional emergent project as-needed support applies across Tasks 1 through 6 for potential Army stakeholders.

All or some of the INSCOM support options are expected to be exercised either concurrently with TOA or at any point in the TO period of performance with advance notification. It is also possible that none of the options will be exercised.